# Account Data Compromise User Guide

25 February 2011

# Notices

**Proprietary Rights**

The information contained in this document is proprietary and confidential to MasterCard International Incorporated, one or more of its affiliated entities (collectively "MasterCard"), or both.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of MasterCard.

**Trademarks**

Trademark notices and symbols used in this document reflect the registration status of MasterCard trademarks in the United States. Please consult with the Customer Operations Services team or the MasterCard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

**Billing**

For printed documents, MasterCard will bill principal members. Please refer to the appropriate *MasterCard Consolidated Billing System* (MCBS) document for billing-related information.

**Information Available Online**

MasterCard provides details about the standards used for this document—including times expressed, language use, and contact information—on the Member Publications Support page available on MasterCard OnLine®. Go to Member Publications Support for centralized information.

**Translation**

A translation of any MasterCard manual, bulletin, release, or other MasterCard document into a language other than English is intended solely as a convenience to MasterCard members and other customers. MasterCard provides any translated document to its members and other customers "AS IS" and makes no representations or warranties of any kind with respect to the translated document, including, but not limited to, its accuracy or reliability. In no event shall MasterCard be liable for any damages resulting from members' and other customers' reliance on any translated document. The English version of any MasterCard document will take precedence over any translated version in any legal proceeding.

**Publication Code**

ADC

©2009–2011 MasterCard. Proprietary. All rights reserved.

# Summary of Changes, 25 February 2011

This document reflects changes since the 20 August 2010 *Account Data Compromise User Guide*. To locate these changes online, on the Adobe toolbar, click Find. In the Find box, type *chg*, and then press ENTER. To move to the next change, press ENTER again.

| Description of Change | Where to Look |
|---|---|
| Table list of forensic investigators has been replaced with a link to the PCI Security Standards Web site that identifies PCI-approved PCI Forensic Investigators (PFIs). | Appendix B |

©2009–2011 MasterCard. Proprietary. All rights reserved.

# Table of Contents


**Chapter 1 Introduction ..... 1-i**

1.1 Purpose ..... 1-1

1.2 ADC Event Time line ..... 1-1

1.3 Contact Information ..... 1-1

**Chapter 2 Reporting an ADC or Potential ADC ..... 2-i**

2.1 Overview ..... 2-1

2.2 ADC Event Reporting Using MasterCard Alerts ..... 2-2

2.3 ADC Reporting Form ..... 2-2

2.3.1 Guidelines—General Instructions ..... 2-3

2.3.2 Section A—General Instructions ..... 2-3

2.3.3 Attachments—General Instructions ..... 2-5

2.4 ADC Event Reporting without the Use of MasterCard Alerts ..... 2-7

2.4.1 Secure Upload ..... 2-8

2.4.2 Secure Upload Access for Members ..... 2-8

2.4.3 Secure Upload Access for Non-members ..... 2-9

2.4.4 Encrypted File Transfer Method ..... 2-9

**Chapter 3 Investigation ..... 3-i**

3.1 Overview ..... 3-1

3.2 ADC Investigation Process ..... 3-1

3.2.1 Section B—Investigation Acknowledgment ..... 3-3

3.2.2 Section C—Investigation Results ..... 3-3

3.3 Engaging a Qualified Incident Response Assessor ..... 3-4

3.4 Forensic Report Submission ..... 3-4

3.5 Financial Responsibility ..... 3-4

**Chapter 4 MasterCard Alerts ..... 4-i**

4.1 Overview ..... 4-1

4.2 Notification of Compromised Accounts Using MasterCard Alerts ..... 4-1

4.3 MasterCard Alerts Quarterly Fees ..... 4-2

4.4 MasterCard Alerts User Profile ..... 4-2

4.5 MasterCard Alerts—Noncompliance Assessments ..... 4-3

4.6 MasterCard Alerts License ..... 4-4


©2009–2011 MasterCard. Proprietary. All rights reserved.

**Chapter 5 System to Avoid Fraud Effectively (SAFE) Reporting ..... 5-i**

5.1 Overview ..... 5-1

**Chapter 6 Operational Reimbursement and Fraud Recovery ..... 6-i**

6.1 Overview ..... 6-1

6.2 Acquirer Preliminary Estimate of Potential Financial Responsibility ..... 6-2

6.3 ADC Operational Reimbursement ..... 6-3

6.3.1 ADC Operational Reimbursement Factors ..... 6-3

6.3.2 ADC Operational Reimbursement Administrative Fee ..... 6-5

6.3.3 ADC Operational Reimbursement—BIN Reports ..... 6-6

6.3.4 ADC Operational Reimbursement—Reimbursement Notification ..... 6-7

6.3.5 ADC Operational Reimbursement—Acquirer Responsibility Cap ..... 6-7

6.4 ADC Fraud Recovery ..... 6-8

6.4.1 ADC Fraud Recovery Factors ..... 6-8

6.4.2 ADC Fraud Recovery—Administrative Fee ..... 6-10

6.4.3 ADC Fraud Recovery—BIN Reports ..... 6-10

6.4.4 ADC Fraud Recovery—Reimbursement Notification ..... 6-11

6.4.5 ADC Fraud Recovery—Acquirer Responsibility Cap ..... 6-12

**Chapter 7 Financial Settlement ..... 7-i**

7.1 Overview ..... 7-1

7.2 Operational Reimbursement Notification ..... 7-1

7.3 Operational Reimbursement—Responsible Member Responsibility ..... 7-1

7.4 Operational Reimbursement Billing Event Codes ..... 7-1

7.5 Fraud Recovery—Reimbursement Notification ..... 7-2

7.6 Fraud Recovery—Responsible Member Responsibility ..... 7-2

7.7 Fraud Recovery Billing Events ..... 7-2

7.8 Event Case Management ..... 7-3

**Appendix A Required ADC File Format ..... A-i**

Required ADC File Format ..... A-1

**Appendix B Forensic Investigators Approved by MasterCard ..... B-i**

Forensic Investigators Approved by MasterCard ..... B-1

**Appendix C ADC Event Status Report ..... C-i**

ADC Event Status Report ..... C-1

ADC Investigation Weekly Status Report ..... C-1

©2009–2011 MasterCard. Proprietary. All rights reserved.

**Appendix D Incident Report ..... D-i**

Incident Report ..... D-1

**Appendix E Acquirer Responsibility Pre-estimate Letter ..... E-i**

Acquirer Responsibility Pre-estimate Letter ..... E-1

**Appendix F MasterCard Resources ..... F-i**

MasterCard Information Manual ..... F-1

Quarterly Member Reporting ..... F-1

MasterCard Registration Program (MRP) ..... F-1

System to Avoid Fraud Effectively (SAFE) ..... F-1

MasterCard OnLine ..... F-2

MasterCard Alerts ..... F-2

MasterCard Magnetic Stripe ADC At-risk Accounts Alerts Service ..... F-2

**Appendix G MasterCard Alerts and ADC Reporting Form Field Definitions ..... G-i**

Section A, Page 1—Field Descriptions ..... G-1

Section A, Page 2—Field Descriptions ..... G-2

**Appendix H MasterCard Alerts ADC Reporting Form Status Codes ..... H-i**

MasterCard Alerts ADC Reporting Form Status Codes ..... H-1

**Appendix I MasterCard Alerts ADC Section C—Investigation Results ..... I-i**

Field Definitions ..... I-1

Merchant Information ..... I-1

POS Equipment Details ..... I-1

Investigative Results ..... I-1

Law Enforcement Contact Information ..... I-1

Merchant Investigation Results ..... I-2

Preventive Measures Implemented ..... I-2

©2009–2011 MasterCard. Proprietary. All rights reserved.

# Chapter 1 Introduction

*This chapter explains the purpose of this user guide, describes the ADC event time line, and provides contact information for various regional offices of the MasterCard Customer Operations Team.*

1.1 Purpose ..... 1-1

1.2 ADC Event Time line ..... 1-1

1.3 Contact Information ..... 1-1

©2009–2011 MasterCard. Proprietary. All rights reserved.

# 1.1 Purpose

The MasterCard *Account Data Compromise User Guide* sets forth instructions for MasterCard members, merchants, and agents, including but not limited to member service providers and data storage entities regarding processes and procedures relating to the administration of the MasterCard Account Data Compromise (ADC) program.

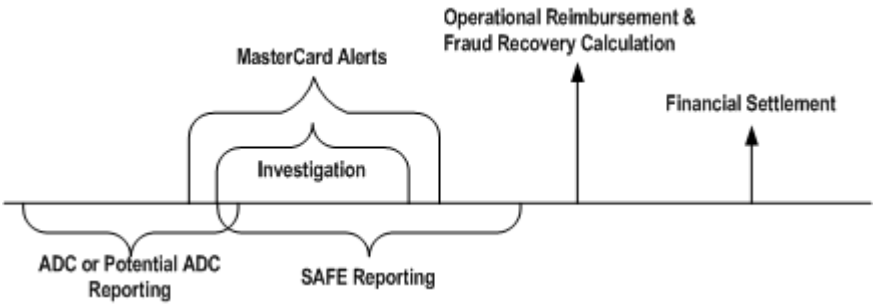
The MasterCard Standards relating to ADC events or potential ADC events are set forth in section 10.2, Account Data Compromise Events, of the *Security Rules and Procedures* manual.

As defined in the MasterCard *Security Rules and Procedures* section 10.2 an "Account Data Compromise Event" or "ADC Event" means an occurrence that results, directly or indirectly, in the unauthorized access to or disclosure of MasterCard account data. A "potential Account Data Compromise Event" or "potential ADC Event" means an occurrence that could result, directly or indirectly, in the unauthorized access to or disclosure of MasterCard account data.

# 1.2 ADC Event Time line

The ADC event time line set forth below depicts the life cycle of an ADC event or potential ADC event. This guide depicts each of the individual phases and steps associated with the administration of a typical ADC event or potential ADC event.

Given the nature and complexity of ADC events or potential ADC events, it is important to note that this guide is not intended to set forth the process and procedures associated with every possible ADC event or potential ADC event, and as such, the guide is subject to change at the discretion of MasterCard.




# 1.3 Contact Information

For contact information, refer to the Information Available Online section of the Notices page.

©2009–2011 MasterCard. Proprietary. All rights reserved.

# Chapter 2 Reporting an ADC or Potential ADC

*This chapter discusses security vulnerabilities in payment processing environments and indicators of a security breach, unauthorized activity, or possible signs of misuse within a payment environment, which may be indicative of an ADC event or potential ADC event.*


2.1 Overview ..... 2-1

2.2 ADC Event Reporting Using MasterCard Alerts ..... 2-2

2.3 ADC Reporting Form ..... 2-2

2.3.1 Guidelines—General Instructions ..... 2-3

2.3.2 Section A—General Instructions ..... 2-3

2.3.3 Attachments—General Instructions ..... 2-5

2.4 ADC Event Reporting without the Use of MasterCard Alerts ..... 2-7

2.4.1 Secure Upload ..... 2-8

2.4.2 Secure Upload Access for Members ..... 2-8

2.4.3 Secure Upload Access for Non-members ..... 2-9

2.4.4 Encrypted File Transfer Method ..... 2-9


©2009–2011 MasterCard. Proprietary. All rights reserved.

# 2.1 Overview

Security vulnerabilities in an existing payment processing environment may not immediately be known; however, there may be indicators of a security breach, unauthorized activity, or possible signs of misuse within the payment environment that may be indicative of an ADC event or potential ADC event. The following examples of ADC events should not be considered a comprehensive or exhaustive list:

- Internet connections from non–business-related IP addresses[1] or inbound Internet connections originating from countries without a business relationship to the potentially compromised entity or outbound Internet connections to non–business-related IP addresses or countries or both
- Log-in activity from unknown or inactive user IDs or excessive login activity from user IDs
- Presence of malware, suspicious files, or executables and programs in an environment, or presence of unusual activity or volume in network systems
- SQL injection activity on Web-facing systems
- POS terminals and ATM devices showing signs of tampering
- Key-logger found
- Card-skimming devices found
- Lost, stolen, or misplaced sales receipt
- Lost, stolen, or misplaced payment card data
- Lost, stolen, or misplaced computers, laptops, hard drives, or other devices that contain MasterCard payment card data
- Files containing MasterCard account data mistakenly transmitted to an unauthorized party

If activity associated with any of the above evidence or information is uncovered, it is necessary to immediately conduct an investigation and to comply with MasterCard *Security Rules and Procedures* section 10.2.2 and procedures defined in this guide.

1. An IP address that is not recognized by the entity in question as being an IP address that would need access to the entity's network.

©2009–2011 MasterCard. Proprietary. All rights reserved.

# 2.2 ADC Event Reporting Using MasterCard Alerts

For information about the required member roles, responsibilities, and associated time frames in response to an ADC event or potential ADC event, refer to the MasterCard *Security Rules and Procedures* Manual, section 10.2.

Members should use the ADC Reporting Form located in MasterCard Alerts to report all types of ADC events or potential ADC events to MasterCard, in compliance with Section 10.2 of the MasterCard *Security Rules and Procedures* manual. Events include but are not limited to the following:

- A member or its agents becoming aware of an ADC event or potential ADC event in or affecting any system or environment of the member or its agent
- An issuer experiencing elevated fraud or suspecting an ADC event or potential ADC event

If the member does not have access to MasterCard Alerts, refer to 2.4 ADC Event Reporting without the Use of MasterCard Alerts.

# 2.3 ADC Reporting Form

The ADC Reporting Form is to be used for reporting and providing information about an ADC or potential ADC event.

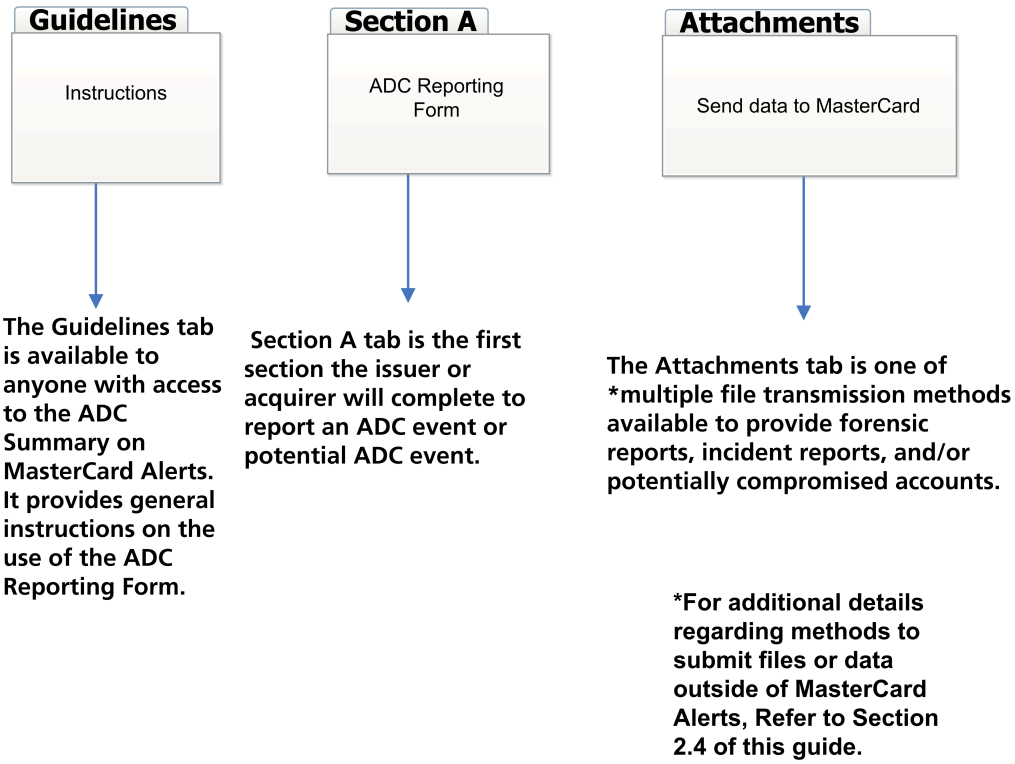
Registered users can access the ADC Reporting Form by following these steps:

1. Enter MasterCard OnLine®.
2. Point to **My Products** in the **Products** drop-down list.
3. Select **MasterCard Alerts**.
4. Read the disclaimer, and then click **Accept** if you accept the terms.
5. Click **ADC Summary**.
6. Click the **ADC Reporting Form** button, located below the main tabs at the top of the ADC Summary page. The ADC Reporting Form field definitions are located in Appendix G, MasterCard Alerts and ADC Reporting Form Field Definitions.

The ADC Reporting Form consists of the following tabs:

- Guidelines
- Section A (As the investigation proceeds, Sections B and C also will be displayed.)
- Attachments

©2009–2011 MasterCard. Proprietary. All rights reserved.


Guidelines
Instructions
Section A
ADC Reporting Form
Attachments
Send data to MasterCard
The Guidelines tab is available to anyone with access to the ADC Summary on MasterCard Alerts. It provides general instructions on the use of the ADC Reporting Form.
Section A tab is the first section the issuer or acquirer will complete to report an ADC event or potential ADC event.
The Attachments tab is one of *multiple file transmission methods available to provide forensic reports, incident reports, and/or potentially compromised accounts.
*For additional details regarding methods to submit files or data outside of MasterCard Alerts, Refer to Section 2.4 of this guide.

The header information (above the three tabs) shows the Merchant Name, Status, and Tracking Number fields. The system automatically assigns the Tracking Number when the form is first opened and is used to track every ADC submission throughout the life cycle of the event. The Merchant Name field is blank when this form is created but contains the merchant's name if the form has previously been saved as a draft or submitted to MasterCard. If your MasterCard Alerts profile contains only one ICA, that ICA will be shown. Otherwise, click the selection button ▼ to select the ICA you want to use for this report.

## 2.3.1 Guidelines—General Instructions

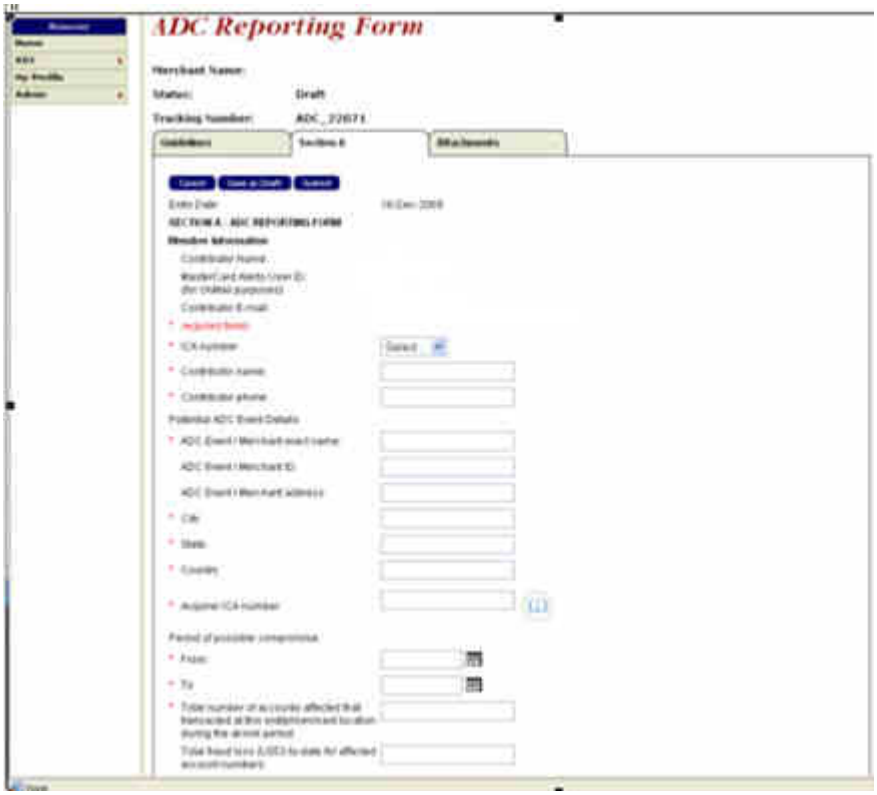
The Guidelines tab contains the general instructions for completing the ADC Reporting Form. It also contains links to MasterCard ADC Rules, the *ADC User Guide*, ADC Reporting Form and Investigation Instructions, the Incident Report, the ADC Event Status Report, ADC File Format, and Security Guidelines for Merchants.

## 2.3.2 Section A—General Instructions

The requestor must complete all the applicable data fields in Section A. If the information is unknown, enter UNKN. If the data element or question is not applicable to the ADC event being reported, enter N/A. Omitting fields may delay the investigation or the applicable next steps of the event.

The following is an illustration of Section A.

©2009–2011 MasterCard. Proprietary. All rights reserved.



©2009–2011 MasterCard. Proprietary. All rights reserved.

The ADC Form field definitions are located in Appendix G, MasterCard Alerts and ADC Reporting Form Field Definitions. Documents may be attached to Section A by clicking either **Upload File(s)** button and following the instructions. An ADC Incident Report must be attached to the ADC Reporting Form when an acquirer makes its initial report of an ADC event or potential ADC event. An issuer usually does not have enough information to complete an Incident Report.Appendix D, Incident Report provides a link to the Incident Report form, or the member may "cut and paste" the form from the appendix into a Word document. Attach any additional documents that more fully describe the scope and nature of the ADC event, such as a forensic report or other description of the ADC event or potential ADC event and its impact. The attachment feature is further explained in 2.3.3 Attachments—General Instructions.

**NOTE**

**Issuers are required to report actual fraudulent transactions to SAFE.**

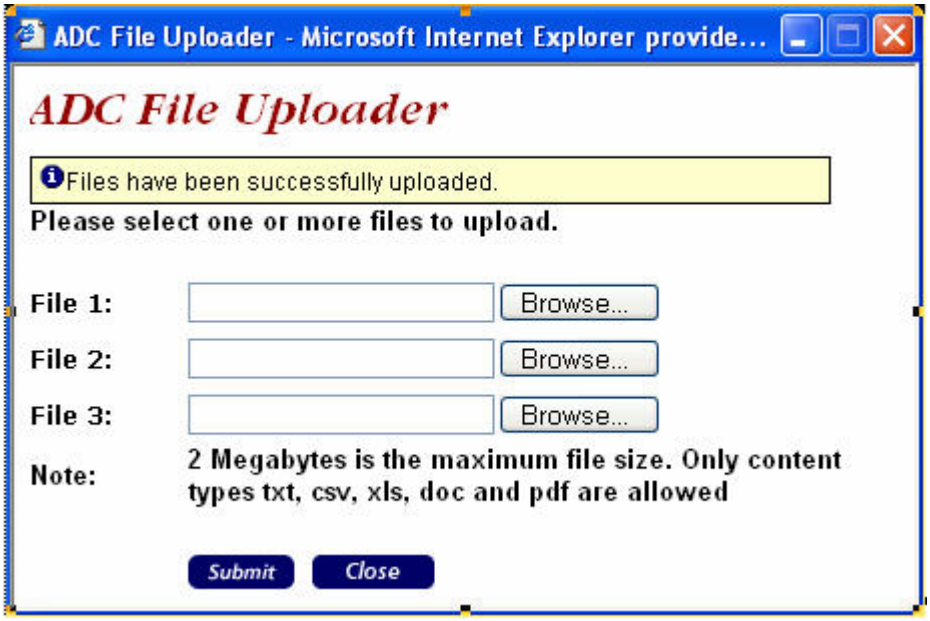
## 2.3.3 Attachments—General Instructions

The following is a representation of the Account Data Compromise Form Attachments tab.

Click **Upload File** below the verbiage, "Transaction information is provided in attached document" to attach documents to Section A.

The following screen becomes available for attachments while the user is in Section A:

©2009–2011 MasterCard. Proprietary. All rights reserved.




Follow the instructions on the ADC File Uploader screen. Click **Submit** to make the files available under the Attachments tab. Enter or paste the necessary files in the **File 1** field. If you prefer, click on the corresponding Browse button to locate the files for uploading. Repeat this process if you have up to two additional files. Click **Submit** to upload the files. Once the files have been uploaded, the message "File(s) have been attached" is displayed. Repeat this process until all desired files are attached. The files are now available under the Attachments tab.

If the at-risk account numbers are readily available, create a file of all at-risk MasterCard or Maestro account numbers as defined in Appendix A, Required ADC File Format. This obligation applies regardless of how or why such account numbers were received, processed, or stored, including, by way of example and not limitation, in connection with or relating to a credit, debit (signature- or PIN-based) proprietary, or any other kind of payment transaction, incentive, or reward program. The required BIN ranges start with 510000 to 559999 and 670000 to 679999.

If the at-risk account numbers are not readily available, they may be submitted at a later date using Section C of the ADC Reporting Form.

Although MasterCard will accept all submissions, regardless of the format used, MasterCard will reformat any file not submitted as defined in Appendix A, Required ADC File Format and may assess a reformatting fee to the requestor according to the number of submitted accounts that need to be reformatted. The fee (described in the following table) will be debited using the MasterCard Consolidated Billing System (MCBS).

©2009–2011 MasterCard. Proprietary. All rights reserved.

| Number of Reformatted Accounts | Fee (USD) | Fee (BRL)[2] | MCBS Billing Event |
|---|---|---|---|
| More than 3,000,000 | USD 5,000 | BRL 13,000 | 2SC1207 |
| 1,000,001–3,000,000 | USD 3,500 | BRL 9,100 | 2SC1206 |
| 500,001–1,000,000 | USD 2,000 | BRL 5,200 | 2SC1205 |
| 100,001–500,000 | USD 1,000 | BRL 2,600 | 2SC1204 |
| 1–100,000 | USD 500 | BRL 1,300 | 2SC1203 |

Section A can be saved in draft form in MasterCard Alerts before it is electronically submitted to MasterCard.

The ADC Reporting Form entry must be "submitted" before MasterCard can process the report. This is done by clicking **Submit** at the bottom of Section A. MasterCard recommends the form be saved as a draft before stepping away from the application for even a few minutes. No information will be saved if **Cancel** is clicked.

## 2.4 ADC Event Reporting without the Use of MasterCard Alerts

If a member does not have access to MasterCard Alerts, at-risk account data and the Incident Report form may be submitted to MasterCard using one of the following methods:

- Secure Upload
- Secure Upload—URL and password (available only to MasterCard OnLine® non-members)
- Encrypted File Transfer Method

When at-risk account numbers are available, submit them in separate files, along with the Incident Report, to MasterCard, using Secure Upload or the File Transfer Method. For additional information regarding the Incident Report, refer to Appendix D, Incident Report.

If at-risk accounts are not readily available, submit the Incident Report to account_data_compromise@mastercard.com.

Account data should never be sent without being encrypted before transmission. Each method of transport described in this guide offers a method of securely transferring account data.

2. For Brazilian members that have entered into a specific service agreement with the MasterCard local operating subsidiary in Brazil, MasterCard Brasil Soluções de Pagamento Ltda. ("Permanent Establishment—PE"), prices are denominated in Brazilian Real (BRL). All other members will be billed in USD at the USD rate.

©2009–2011 MasterCard. Proprietary. All rights reserved.

For the required file format, refer to Appendix A, Required ADC File Format. All files containing compromised or potentially compromised account data must be submitted in the file format defined in this guide. MasterCard will accept all submissions regardless of the format used, and MasterCard will reformat any file not submitted as defined in Appendix A, Required ADC File Format. For the reformatting fee, refer to 2.3.3 Attachments—General Instructions. The fee may be charged to the requestor.

## 2.4.1 Secure Upload

The Secure Upload feature allows for the secure file transfer of compromise information through a secure MasterCard Web site. This feature expedites the receipt and delivery of at-risk account information. A brief description characterizing the provided data is required along with the account data.

Consider the following when uploading data using Secure Upload:

- The file size is limited to 50 megabytes (MB).
- MasterCard prefers text (*.txt) and Excel® (*.xls) file formats for at-risk accounts.
- MasterCard prefers text, .pdf, or Word® documents for communications related to investigations.

Secure Upload is available through MasterCard OnLine® for MasterCard members and non-members.

MasterCard will provide temporary access for non-members to Secure Upload for the secure transmission of compromised accounts.

## 2.4.2 Secure Upload Access for Members

To obtain access to the Secure Upload product, refer to the Product Catalog on MasterCard OnLine

1. Navigate to www.mastercardonline.com.
2. Log on using your **User ID** and **Security Information**.
3. At the top left of the home page under the **Products** menu, click **Order Products** to open the MasterCard OnLine® Product Catalog.
4. Under the **Shop** tab, select **All Products** from the **View** drop-down menu.
5. In the **Products** list, scroll down to click on **Secure Upload**.
6. Click **Add to Cart** to submit a request for the Secure Upload product.
7. Complete the checkout process.

©2009–2011 MasterCard. Proprietary. All rights reserved.

### 2.4.3 Secure Upload Access for Non-members

Non-members that need to submit account data to MasterCard can do so through Secure Upload using a URL and password. Send an e-mail message to mastercard_alerts_administrator@mastercard.com requesting access using the URL. Include the following information in your e-mail message:

- Case number or potentially compromised entity name
- Submitter's contact information (name, title, organization, and phone number)

### 2.4.4 Encrypted File Transfer Method

Members that cannot submit files using Secure Upload must send such files encrypted using WinZip® (or similar encryption tool) to help ensure that the account data is secure while in transit. Send all such encrypted files to account_data_compromise@mastercard.com.

Encryption must comply with industry standards FIPS SP800-57 Part 1.

©2009–2011 MasterCard. Proprietary. All rights reserved.

# Chapter 3 Investigation

*This chapter discusses the processes pertaining to the investigation of an ADC event or a potential ADC event.*


3.1 Overview ..... 3-1

3.2 ADC Investigation Process ..... 3-1

3.2.1 Section B—Investigation Acknowledgment ..... 3-3

3.2.2 Section C—Investigation Results ..... 3-3

3.3 Engaging a Qualified Incident Response Assessor ..... 3-4

3.4 Forensic Report Submission ..... 3-4

3.5 Financial Responsibility ..... 3-4


©2009–2011 MasterCard. Proprietary. All rights reserved.

# 3.1 Overview

It is the expectation of MasterCard that each responsible member follow the rules as set forth in section 10.2.2 of the MasterCard *Security Rules and Procedures* manual pertaining to the investigation of an ADC event or a potential ADC event. The responsible member is held accountable for achieving resolution of all outstanding issues to the satisfaction of MasterCard.

# 3.2 ADC Investigation Process

As defined in 2.2 ADC Event Reporting Using MasterCard Alerts, MasterCard requires an ADC Reporting Form to be completed and submitted through MasterCard Alerts. Once the ADC Reporting Form is submitted, the requestor should monitor the ADC Reporting Form status codes.

**NOTE**

**Submission of an investigation request using the ADC Reporting Form does not mean an investigation is in process.**

If MasterCard receives a report of a potential ADC event or ADC event, MasterCard may validate the information shared by the member using the ADC Reporting Form. When appropriate, MasterCard will work with the acquirers of record to achieve compliance with MasterCard rules.

If MasterCard determines further investigative is warranted, MasterCard will send an e-mail to the security contact for the ICA, as defined in the *MasterCard Member Information Manual* (MIM) MasterCard OnLine® profile, notifying the acquirer that an acknowledgement of a potential ADC event is pending in MasterCard Alerts ADC Reporting Form, Section B. For instruction, refer to Chapter 2, Reporting an ADC or Potential ADC

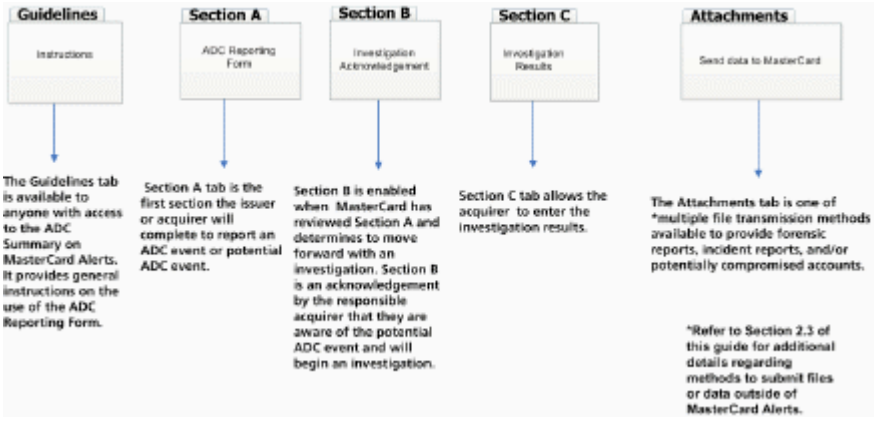
Registered users from the responsible acquirer must access Section B of the ADC Reporting Form within five business days of the e-mail by navigating as follows:

1. Enter MasterCard OnLine.
2. Point to **My Products** in the **Products** drop-down list.
3. Select **MasterCard Alerts**.
4. Click **Yes** in the Security Warning dialoge box. The MasterCard Alerts disclaimer page opens.
5. Read the disclaimer, and then click **Accept** if you accept the terms.

©2009–2011 MasterCard. Proprietary. All rights reserved.

6. On the MasterCard Alerts home page, click **ADC Summary**.
7. From the ADC Summary, select the tracking number that corresponds to the tracking number provided in the e-mail notification.
8. Select the Section B tab and complete the four data fields asking for the acquirer's contact information for this investigation.
9. To satisfy MasterCard response requirements, click **Save**. To keep the acknowledgment form blank, click **Cancel**.

MasterCard Alerts will enable Section B for the acquirer to review and acknowledge intent to investigate. In addition to Section B, MasterCard Alerts will display other sections that are used in various stages of this process as outlined in the flow below.


Guidelines
Instructions
The Guidelines tab is available to anyone with access to the ADC Summary on MasterCard Alerts. It provides general instructions on the use of the ADC Reporting Form.
Section A
ADC Reporting Form
Section A tab is the first section the issuer or acquirer will complete to report an ADC event or potential ADC event.
Section B
Investigation Acknowledgement
Section B is enabled when MasterCard has reviewed Section A and determines to move forward with an investigation. Section B is an acknowledgement by the responsible acquirer that they are aware of the potential ADC event and will begin an investigation.
Section C
Investigation Results
Section C tab allows the acquirer to enter the investigation results.
Attachments
Send data to MasterCard
The Attachments tab is one of *multiple file transmission methods available to provide forensic reports, incident reports, and/or potentially compromised accounts.
*Refer to Section 2.3 of this guide for additional details regarding methods to submit files or data outside of MasterCard Alerts.

The contributor will know that MasterCard has initiated an investigation if the ADC Summary or the ADC Reporting Form status changes to **Open** or **Investigating**.

©2009–2011 MasterCard. Proprietary. All rights reserved.

### 3.2.1 Section B—Investigation Acknowledgment

Clicking the **Save** button changes the case status to "Investigating" and the status can be seen by the person submitting this form.

### 3.2.2 Section C—Investigation Results

The investigation results must be submitted to MasterCard within 30 business days of the acquirer receiving the MasterCard investigation acknowledgment. The acquirer must use Section C to submit its investigation results to MasterCard.

Acquirers may be assessed a non-compliance penalty for failure to comply with investigation time frames as set forth in section 10.2 of the MasterCard *Security Rules and Procedures* manual.

To access Section C users must navigate as follows:

1. Enter MasterCard OnLine.
2. Click **MasterCard Alerts**.
3. Select **ADC Summary**.
4. Select the tracking number that corresponds to the appropriate investigation.
5. Select the **Section C** tab.

Five components in Section C must be completed by the acquirer:

1. Merchant Information
2. POS Equipment Details
3. Investigation Results
4. Law enforcement contact information
5. Merchant Investigation Results

©2009–2011 MasterCard. Proprietary. All rights reserved.

All required fields denoted by an asterisk (*) must be completed. If the information is unknown, enter **UNKN**, or if it is not applicable to the ADC event, enter **N/A**.

For Section C field definitions, refer to Appendix I, MasterCard Alerts ADC Section C—Investigation Results.

## 3.3 Engaging a Qualified Incident Response Assessor

For the process of engaging a qualified incident response assessor (QIRA) to conduct a forensic investigation, refer to the *Security Rules and Procedures* manual, section 10.2.2.

MasterCard *Security Rules and Procedures*, section 10.2.2.1, item e states, "Prior to the commencement of such QIRA's investigation, the Member must notify MasterCard of the proposed scope and nature of the investigation and obtain preliminary approval of such proposal by MasterCard or, if such preliminary approval is not obtained, of a modified proposal acceptable to MasterCard."

The documentation relating to the scope should be attached to the ADC Reporting Form in MasterCard Alerts for MasterCard review and approval.

## 3.4 Forensic Report Submission

The preliminary and final forensic reports may be submitted by e-mail to forensic_reports@mastercard.com. The forensic report should be password-protected. The password is to be communicated to the case manager independent of the e-mail message containing the forensic report.

## 3.5 Financial Responsibility

If MasterCard determines that operational reimbursement (OR) or fraud recovery (FR) or both might be invoked for a specific ADC event or potential ADC event, MasterCard will estimate the total OR and FR amounts the responsible acquirer may owe, using the data available as of the calculation date. Actual liability may be different.

MasterCard will notify the responsible acquirer by e-mail to the parent ICA Security Contact (as defined in the MIM) of their potential financial responsibility. See the "Acquirer Responsibility Pre-estimate Letter" sample in Appendix E, Acquirer Responsibility Pre-estimate Letter. Note that this "Pre-estimate Letter" is a preliminary estimate of the responsible member's financial responsibility. The actual financial responsibility will depend on the results of the ADC event investigation.

©2009–2011 MasterCard. Proprietary. All rights reserved.

# Chapter 4 MasterCard Alerts

*This chapter describes the usage of MasterCard Alerts.*

4.1 Overview ..... 4-1

4.2 Notification of Compromised Accounts Using MasterCard Alerts ..... 4-1

4.3 MasterCard Alerts Quarterly Fees ..... 4-2

4.4 MasterCard Alerts User Profile ..... 4-2

4.5 MasterCard Alerts—Noncompliance Assessments ..... 4-3

4.6 MasterCard Alerts License ..... 4-4

©2009–2011 MasterCard. Proprietary. All rights reserved.

# 4.1 Overview

Each principal and associated member must be licensed for MasterCard Alerts. To be eligible for Operational Reimbursement and Fraud Recovery, as set forth under section 10.2.4.3 in the MasterCard *Security Rules and Procedures*, a member must have and maintain an active MasterCard Alerts license for all its member IDs/ICA numbers.

A member must ensure that any registered third-party processor (TPP), member service provider (MSP), or independent service organization (ISO) authorized to manage MasterCard Alerts on behalf of the member, has access to MasterCard Alerts.

# 4.2 Notification of Compromised Accounts Using MasterCard Alerts

When MasterCard determines that account data may be at risk as the result of an ADC event or potential ADC event, MasterCard may publish a MasterCard Alert to notify issuers of the accounts that may be at risk.

MasterCard also may contact the affected issuers by e-mail to notify them of a new MasterCard Alert. The e-mail notification instructs the issuer to log on to MasterCard Alerts to obtain a listing of compromised or potentially compromised accounts and a description of the ADC event or potential ADC event.

Members may elect not to receive MasterCard Alerts e-mail notifications by sending an e-mail to mastercard_alerts_administrator@mastercard.com with "Discontinue Alerts E-mail Notifications" in the subject line.

Users of the MasterCard Alerts tool who are not receiving MasterCard Alerts e-mail notifications may begin to receive these e-mail notifications by sending an e-mail to mastercard_alerts_administrator@mastercard.com with "Sign up for Alerts E-mail Notifications" in the subject line.

**NOTE**

**MasterCard Alerts e-mail notification uses the e-mail address located in the user's MasterCard OnLine® user profile.**

©2009–2011 MasterCard. Proprietary. All rights reserved.

# 4.3 MasterCard Alerts Quarterly Fees

MasterCard will assess a quarterly license fee at the parent member ID/ICA number level through MCBS for access to MasterCard Alerts. Because of privacy laws, affiliates without their own ICA must obtain information from their processor.

The fees are calculated according to the total number of accounts (including both open and blocked accounts) reported by each member in the Quarterly Member Report (QMR) for the preceding quarter.

**Fee Structure in Regions Other than the Europe Region**

| Tier | Total Accounts | Quarterly Fee |
|---|---|---|
| 1 | More than 2,000,000 | USD 5,000 |
| 2 | 400,000–2,000,000 | USD 2,000 |
| 3 | Less than 400,000 | USD 300 |

**Fee Structure in the Europe Region**

| Tier | Total Accounts | Quarterly Fee |
|---|---|---|
| 1 | More than 2,000,000 | EUR 5,000 |
| 2 | 400,000–2,000,000 | EUR 2,000 |
| 3 | Less than 400,000 | EUR 300 |

**MasterCard Alerts Licensing—Billing Events**

| Billing Event No. | Billing Event Description |
|---|---|
| 2SC1357 | MC Alerts licensing fee—USD |
| 2KS13575 | MC Alerts licensing fee—Euros |
| 2SC1357 | MC Alerts licensing fee—Reals |

# 4.4 MasterCard Alerts User Profile

New members have 30 calendar days from the initial date of membership to obtain a license.

©2009–2011 MasterCard. Proprietary. All rights reserved.

If a member needs to update its MasterCard Alerts user profile with a new e-mail address or name to update its contact information (e-mail address, name, or street address) the member should change its MasterCard OnLine user profile. To update its ICAs listed in its MC Alerts profile, member should complete an update request. To delete its MasterCard OnLine user profile, the member must complete a termination request on MasterCard OnLine or add or delete ICAs, or terminate its MasterCard Alerts access. Any changes will take between one and three business days to be reflected in the MasterCard Alerts profile. To make changes to the MasterCard Alerts profile, the member must:

1. Navigate to MasterCard OnLine.
2. Log in to MasterCard OnLine by entering your **User ID** and **Security Information**.
3. From the **Products** menu on the left of your screen, click **Order Products** to open the **MasterCard OnLine—Product Catalog** window.
4. From the **Shop** tab, select the **All Products** option button.
5. Search the list alphabetically.
6. Click **MasterCard Alerts**.
7. Click **Subscribe Now** located in the lower half of the window.
8. Complete the request form and submit for processing.

**NOTE**

**Members should monitor their MasterCard Alerts user ID to ensure access continuity.**

# 4.5 MasterCard Alerts—Noncompliance Assessments

MasterCard may impose the following noncompliance assessments on members that are not licensed to access MasterCard Alerts.

| Noncompliance | Assessment |
|---|---|
| Existing members not licensed to access MasterCard Alerts | Members will have 30 calendar days from the date of notice of noncompliance to become licensed. |
| | If the member is not licensed within 30 calendar days of the date of notice, MasterCard may assess the member USD 5,000 for each month of noncompliance. |
| New members not licensed to access MasterCard Alerts | Members will have 30 calendar days from the initial date of membership to become licensed. |
| | If the member is not licensed within 30 calendar days, MasterCard may assess the member USD 5,000 for each month of noncompliance. |

**NOTE**

**The effective "date of notice of compliance" is the date that an e-mail notice is sent to the Principal Contact and Security Contact of the member listed in the most recent edition of the *MasterCard MIM* MasterCard OnLine profile.**

©2009–2011 MasterCard. Proprietary. All rights reserved.

# 4.6 MasterCard Alerts License

New members have 30 calendar days from the initial date of membership to obtain a license.

Member staff must request a license for product access via the MasterCard OnLine Product Catalog on MasterCard OnLine in accordnce with the following instructions:

1. Navigate your browser to www.mastercardonline.com.
2. Log in to MasterCard OnLine by entering your **User ID** and **Security Information**.
3. From the **Products** menu on the left of your screen, click **Order Products** to open the **MasterCard OnLine–Product Catalog** window.
4. From the **Shop** tab, select the **All Products** option button.
5. Search the list alphabetically.
6. Click **MasterCard Alerts**.
7. Click **Subscribe Now** located in the lower half of the window.
8. Complete the request form and submit for processing.

**NOTE**

**Members should monitor their MasterCard Alerts user ID to ensure access continuity.**

For instructions on how to register for MasterCard OnLine access, contact the MasterCard Customer Operations Support (COS) team. The contact information for the COS team can be found in section 1.3.

MasterCard will automatically terminate any MasterCard OnLine user who has not logged on to MasterCard Alerts for nine months. The member's MasterCard Alerts license will be terminated at the same time as its MasterCard OnLine user license. Once a MasterCard Alerts license is terminated, users who want to renew their license must apply for a new license following the procedures defined above.

©2009–2011 MasterCard. Proprietary. All rights reserved.

# Chapter 5 System to Avoid Fraud Effectively (SAFE) Reporting

*This chapter describes how the MasterCard Fraud Recovery program interacts with SAFE in the reporting of fraud data and the calculation of incremental fraud.*

5.1 Overview ..... 5-1

©2009–2011 MasterCard. Proprietary. All rights reserved.

# 5.1 Overview

The MasterCard Fraud Recovery program uses POS Entry Mode 80 and 90, counterfeit fraud transaction data that is submitted to SAFE by the issuer when calculating incremental fraud at the parent ICA level. Fraud transaction data submitted to SAFE with a fraud type other than counterfeit and POS entry modes 80 or 90 will be ignored when incremental fraud is being calculated. Additionally, once the Fraud Recovery program completes its calculation, each issuer's fraud recovery reimbursement amount is final.

Section 6.4.1 ADC Fraud Recovery Factors, item number 1, "At-risk Time Frame," provides information about the amount of time for issuers to correctly submit fraud transaction information to SAFE.

Accurate and timely submission of fraud data to SAFE will assist MasterCard in its efforts to reduce fraud through early identification.

Instructions on SAFE usage can be found in the *Complete SAFE Manual*. The *Complete SAFE Manual* is available on the MasterCard Member Publications Web site on the Security/Risk Services Web page.

©2009–2011 MasterCard. Proprietary. All rights reserved.

# Chapter 6 Operational Reimbursement and Fraud Recovery

*This chapter discusses operational reimbursement and fraud recovery.*


6.1 Overview ..... 6-1

6.2 Acquirer Preliminary Estimate of Potential Financial Responsibility ..... 6-2

6.3 ADC Operational Reimbursement ..... 6-3
- 6.3.1 ADC Operational Reimbursement Factors ..... 6-3
- 6.3.2 ADC Operational Reimbursement Administrative Fee ..... 6-5
- 6.3.3 ADC Operational Reimbursement—BIN Reports ..... 6-6
- 6.3.4 ADC Operational Reimbursement—Reimbursement Notification ..... 6-7
- 6.3.5 ADC Operational Reimbursement—Acquirer Responsibility Cap ..... 6-7

6.4 ADC Fraud Recovery ..... 6-8
- 6.4.1 ADC Fraud Recovery Factors ..... 6-8
- 6.4.2 ADC Fraud Recovery—Administrative Fee ..... 6-10
- 6.4.3 ADC Fraud Recovery—BIN Reports ..... 6-10
- 6.4.4 ADC Fraud Recovery—Reimbursement Notification ..... 6-11
- 6.4.5 ADC Fraud Recovery—Acquirer Responsibility Cap ..... 6-12


©2009–2011 MasterCard. Proprietary. All rights reserved.

# 6.1 Overview

MasterCard publishes a Global Security Alert (GSA) announcing the commencement of Operation Reimbursement (OR) or Fraud Recovery (FR) or both for a specific MasterCard Alerts case number. The GSA is published on MasterCard Alerts and the MasterCard Member Publications Web site on MasterCard OnLine®.

Upon publication of a GSA announcing the commencement of OR/FR, an e-mail notification is sent automatically to all MasterCard Alerts users who elect to receive e-mail "alert" notifications.

The GSA announcing the commencement of OR or FR or both establishes a timeline indicating the date on which FR recovery amounts will be calculated. The amount of time the issuer has to enter fraud transaction information into SAFE is determined by the number of accounts in the ADC event as defined below.

| Tier | Minimum Number of Accounts | Maximum Number of Accounts | At-risk Length (Days)[1] |
|---|---|---|---|
| 1 | 5,000,000 | Unlimited | 60 |
| 2 | 1,000,000 | 5,000,000 | 45 |
| 3 | 10,000 | 1,000,000 | 30 |

MasterCard may invoke OR or FR or both on an ADC event that has a minimum of 10,000 at-risk accounts. MasterCard reserves the right to invoke OR or FR or both if fewer than 10,000 accounts are put at risk.

1. The At-Risk Length time frame begins on the date of the first MasterCard Alerts notification. If the alert is published on March 01, and if the case falls into Tier 1, Fraud Recovery would be calculated 60 days after March 01.

©2009–2011 MasterCard. Proprietary. All rights reserved.

# 6.2 Acquirer Preliminary Estimate of Potential Financial Responsibility

MasterCard may provide a preliminary estimate of potential financial responsibility to acquirers based on investigative findings of the case.

When an ADC event exceeds 10,000 or more at-risk accounts MasterCard may send a letter to the acquirer's security contact, listed in the *MasterCard Information Manual* (MIM), with the preliminary estimate. The preliminary estimate is based on the total number of accounts published through MasterCard Alerts for a specific case. The preliminary estimate is a "snapshot in time" of the acquirer's financial responsibility for Operational Reimbursement and Fraud Recovery and may not reflect the acquirer's actual responsibility.

Once the preliminary estimate letter is published, the number of compromised or potentially compromised accounts may increase, leading to a change in potential financial responsibility for the acquirer. MasterCard may periodically provide updated potential financial responsibility information through an updated report to each acquirer's security contact.

The Acquirer Responsibility Report provides a status on all open ADC events for a specific acquirer by ICA. The following example displays two cases; however, if more cases are active, they all will be displayed.

| **ICA** | **Acquirer Name** | | **MM/DD/YY** |
|---|---|---|---|
| **Total Acquirer Responsibility for Operational Reimbursement as of Report Run Date for all Active Cases** | | | |
| **Total Acquirer Responsibility for Fraud Recovery as of Report Run Date for all Active Cases:** | | | |
| **Total Acquirer Responsibility as of Report Run Date:** | | | |
| **Case Number (1):** | XXXXXXXX | **Case Number (2):** | XXXXXXXX |
| **Entity Name:** | Example 1 | **Entity Name:** | Example 2 |
| **Total Accounts:** | xxx,xxx | **Total Accounts:** | xxx,xxx |
| **Type of Case:** | Systemic Breach | **Type of Case:** | Systemic Breach |
| **Operational Reimbursement:** | USD xxx,xxx | **Operational Reimbursement:** | USD xxx,xxx |
| **Fraud Recovery:** | USD xxx,xxx | **Fraud Recovery:** | USD xxx,xxx |
| **Current Responsibility as of Report Run Date:** | USD x,xxx,xxx | **Current Responsibility as of Report Run Date:** | USD x,xxx,xxx |

©2009–2011 MasterCard. Proprietary. All rights reserved.

To request a copy of this report, send an e-mail message to account_data_compromise@mastercard.com. Provide contact name and telephone number and the case number.

# 6.3 ADC Operational Reimbursement

A *Global Security Alert* publication distributed via MasterCard Alerts will notify those affected issuers eligible for ADC operational reimbursement of a specific ADC event. The *Global Security Alert* will contain the date on which the ADC operational reimbursement will be calculated.

The following table summarizes the OR calculation that is explained in detail in the next section

| **OR Pre-calculation Steps** | |
|---|---|
| Determine the size of the issuer as defined in section 6.3.1, item #1. | Tier 2 |
| Identify the type of card issued for each potentially compromised account as defined in section 6.3.1.2. | Magnetic Stripe and Chip |
| **OR Calculation** | |
| Operational Reimbursement Eligible Amount[2] | USD A.00 |
| Less a Fixed Deductible | – USD B.00 |
| Equals Operational Reimbursement Net Amount | = USD D.00 |

## 6.3.1 ADC Operational Reimbursement Factors

The following factors are used to calculate ADC OR. These factors are evaluated by MasterCard at least annually.

- Issuer Size

  The MasterCard OR program uses a tiered approach to reimbursement, which is based on the gross dollar volume at the parent ICA level. The gross dollar volume is obtained from Quarterly Member Report (QMR) for each parent ICA. The gross dollar volume of the issuer is compared with the table below, which then determines the tier into which the issuer falls.

| Tier | Issuer—Gross Dollar Volume |
|---|---|
| 1 | > 1B |
| 2 | 201 MM–1 B |
| 3 | 0–200 MM |

2. The OR eligible amount is based on potentially compromised accounts and the card type determination. See section 6.3.1 for further instruction.

©2009–2011 MasterCard. Proprietary. All rights reserved.

- Card Type Determination

  The cost associated with the re-issuance of a payment card is affected by the type of technology embedded on the card and the volume of reissued cards. MasterCard will determine the card type for each individual account published in MasterCard Alerts to calculate the proper card rate based on issuer tier.

  The ADC OR calculation will afford a different reimbursement rate for each of the following card types:

  – Magnetic Stripe
  – Magnetic Stripe + Chip
  – Magnetic Stripe + *PayPass*
  – Magnetic Stripe + Chip + *PayPass* (Combo)

  To identify the type of technology used, the MasterCard authorization file will be searched for transactions processed 90 days before the MasterCard Alerts date for the alert in which the specific pan was published.

  The following table defines the data elements that will be examined in the authorization record to identify the card types.

| Card Type | DE 22 (Point-of-Service [POS] Entry Mode) | DE 55 (Integrated Circuit Card [ICC] System-related Data |
|---|---|---|
| Magnetic Stripe | 02, 90 | |
| Magnetic Stripe & Chip | 05, 06, 79, 80 | Present |
| Magnetic Stripe & *PayPass* | 91, 92 | |
| Magmetic Stripe & Chip & *PayPass* | 07, 08 | |

  If no transactions are found in the MasterCard authorization transaction record for an at-risk account, the card type will be considered a Magnetic Stripe.

  Once card types have been identified for all at-risk accounts, the operational reimbursement rate, based on the applicable issuer tier (as defined below), will be used for calculating reimbursement.

©2009–2011 MasterCard. Proprietary. All rights reserved.

| Tier | Issuer—Gross Dollar Volume | Mag Stripe | Chip[3] | *PayPass* | Combo[4] |
|---|---|---|---|---|---|
| 1 | > 1B | USD 1.60 | USD 2.38 | USD 2.20 | USD 2.68 |
| 2 | 201 MM–1 B | USD 1.85 | USD 2.63 | USD 2.45 | USD 2.93 |
| 3 | 0–200 MM | USD 2.15 | USD 2.93 | USD 2.75 | USD 3.23 |

- OR Deductible

  A fixed deductible of 43 percent will be applied to the total number of accounts for normal card expirations and accounts published in previous MasterCard Alerts.

  MasterCard considers a soft re-issue a re-issued payment card with the same account number but a new expiration date and CVC 2 code. The OR program uses a three percent factor for soft re-issue. The three percent is added back into the OR total with a net deductible equaling 40 percent.

  For additional information, refer to section 10.2.4.4 of the MasterCard *Security Rules and Procedures* manual.

## 6.3.2 ADC Operational Reimbursement Administrative Fee

MasterCard will retain a three percent administrative fee from an issuer's OR reimbursement to defray costs associated with ADC operational reimbursement.

The updated pricing amounts associated with the OR administration fee are shown in the following table. The OR administrative fee is capped at USD 75,000 and BRU 195,000[5] per case.

**Table 6.1 OR Administrative Fee**

| Pricing | Country | Billing Event |
|---|---|---|
| 3% | U.S. | 2SC1215 |
| 3.51% | Brazil | 2SC1215 |

3. References to Chip in this document refer to Chip cards that support the EMV standard.
4. A "Combo" reimbursement rate will be assigned to a card that contains all three types: magnetic stripe, Chip, and MasterCard® *PayPass*™. For additional information, refer to section 10.2.4.3 of the MasterCard *Security Rules and Procedures* manual.
5. The billing information in the *Account Data Compromise User Guide* applies to customers in Brazil that have entered into a specific services agreement with the MasterCard local operating subsidiary in Brazil (MasterCard Brasil Soluções de Pagamento Ltda. ["MasterCard Brazil"]

©2009–2011 MasterCard. Proprietary. All rights reserved.

The administrative fee is taken from the final operational reimbursement amount and will be identified on the issuer's billing statement under the applicable billing event ID defined below.

## 6.3.3 ADC Operational Reimbursement—BIN Reports

MasterCard will provide ADC OR reports at the bank identification number (BIN) level at no cost. Each report details ADC operational reimbursement for a case by ICA number, for all BINs within the ICA.

To obtain a copy of this report, the issuer must send an e-mail message to account_data_compromise@mastercard.com with the following information:

- Parent ICA number
- MasterCard Alerts Case Number
- Issuer's Contact Name and Phone Number
- Indication of whether this is a one-time request or whether this report should be provided every time OR is invoked for an ADC case

The OR BIN Level report will provide information similar to the following.

**Table 6.2 Operational Reimbursements**

| Parent ICA | Child ICA | BIN | Magstripe Amount USD | Chip Amount USD | *PayPass* Amount USD | Combo Amount USD | Total Amount USD |
|---|---|---|---|---|---|---|---|
| XXXX | | | | | | | |
| | | XXXXX | 10.00 | 5.00 | 1.00 | | 16.00 |
| | | XXXXX | 13.00 | 4.00 | | | 17.00 |
| | | **Sub-total** | **23.00** | **9.00** | **1.00** | | **33.00** |
| | | XXXXX | 10.00 | 5.00 | 1.00 | | 16.00 |
| | | XXXXX | 13.00 | 4.00 | | | 17.00 |
| | | **Sub-total** | **23.00** | **9.00.00** | **1.00** | | **33.00** |
| | | XXXXX | | 5.00 | 1.00 | | 16.00 |
| | | XXXXX | | 4.00 | | | 17.00 |
| | | **Sub-total** | **23.00** | **9.00** | **1.00** | | **33.00** |
| | | **Grand Total** | **69.00** | **27.00** | **3.00** | | **99.00** |

©2009–2011 MasterCard. Proprietary. All rights reserved.

## 6.3.4 ADC Operational Reimbursement—Reimbursement Notification

Once the final ADC operational reimbursement is calculated on a specific ADC event, MasterCard will notify the responsible acquirers by letter of their financial responsibility. MasterCard will debit the acquirer's MCBS account for the amount calculated.

MasterCard will notify each issuer by e-mail to the parent ICA Security Contact (as defined in the MIM) of the total operational reimbursement amount it will receive for a specific ADC event and the date that the Operational Reimbursement amount will be credited to the issuer's MCBS account. See the "Acquirer Responsibility Pre-estimate Letter" sample in Appendix E, Acquirer Responsibility Pre-estimate Letter.

## 6.3.5 ADC Operational Reimbursement—Acquirer Responsibility Cap

Section 10.2.4.2 of the MasterCard *Security Rules and Procedures* manual states that MasterCard "may limit compensation" regarding an ADC event. MasterCard will evaluate the following factors to determine whether a cap is to be invoked for an ADC event:

- Compromised entity PCI Level
- Annual MasterCard sales volume
- Items noted in section 10.2.4.2 of the *Security Rules and Procedures* Manual

MasterCard will exercise discretion to determine whether to limit acquirer financial responsibility if an ADC event is determined to have resulted from a vulnerability at or associated with a PCI Level 3 and 4 merchant.

Any applicable cap is applied to the total OR responsibility and is not applied to any other fees associated with an ADC event.

| **Merchant Cap Example** | | | |
|---|---|---|---|
| MasterCard Merchant Annual Sales | x | 5% | Revised Total OR Responsibility with Cap Applied |

If OR amounts are capped by MasterCard, the revised acquirer total is spread proportionally to all issuers according to the percentage of their originally calculated reimbursement. The following tables demonstrate how the cap is applied.

| | |
|---|---|
| Initial Acquirer Responsibility | USD 39,000 |
| MasterCard Merchant Sales | USD 50,000 |
| PCI Cap 5% | USD 2,500 |

©2009–2011 MasterCard. Proprietary. All rights reserved.

| | Issuer Pay Out | Issuer Pay Out with Cap Applied |
|---|---|---|
| **Issuer 1—90%** | USD 35,100 | USD 2,250 |
| **Issuer 2—5%** | USD 1,950 | USD 125 |
| **Issuer 3—5%** | USD 1,950 | USD 125 |
| **Total** | USD 39,100 | USD 2,500 |

# 6.4 ADC Fraud Recovery

Section 10.2.4.5 of the *Security Rules and Procedures* manual sets forth rules regarding fraud recovery and provides additional information regarding this program. The following summary provides a high-level example of the Fraud Recovery factors used to calculate Fraud Recovery. The FR factors are further described in 6.4.1 ADC Fraud Recovery Factors.

| | |
|---|---|
| CFT fraud on specific case: | USD A.00 |
| Less baseline CFT fraud: | – USD B.00 |
| Equals incremental fraud for case: | = USD C.00 |
| Less fraud losses on duplicate accounts: | – USD D.00 |
| Plus soft reissue: | + USD E.00 |
| Less chargeback deduction: | – USD. F.00 |
| Equals Issuer Fraud Recovery for parent ICA: | = USD G.00 |

The automated ADC FR process replaces the ADC compliance case process. The new process enables an issuer to recover a portion of counterfeit fraud caused by an ADC event. MasterCard will determine an issuer's FR amount related to a particular ADC event. Using accounts published in MasterCard Alerts, MasterCard will calculate a counterfeit baseline by looking at POS 90 and POS 80 counterfeit fraud that was reported to SAFE at the parent ICA level and will calculate the incremental counterfeit fraud associated with an ADC event. MasterCard will no longer accept or process compliance cases related to ADC events.

## 6.4.1 ADC Fraud Recovery Factors

MasterCard uses the following factors to calculate fraud recovery at the parent ICA level. These factors are evaluated by MasterCard at least annually:

- At-risk Time Frame

  The fraud recovery formula uses the eligible accounts disseminated through MasterCard Alerts to determine accounts that are at risk as the result of an ADC event. MasterCard *Security Rules and Procedures* section 10.2.4.5 describes the at-risk time frame.

©2009–2011 MasterCard. Proprietary. All rights reserved.

When the at-risk time frame is known, the fraud recovery formula will use that exact start date and calculate an end date using the following table.

If the fraud recovery time frame is not known, the start date will begin 365 days before the date the first MasterCard Alert associated with the case was published and calculate the end date using the following table.

| Tier | Minimum Number of Accounts | Maximum Number of Accounts | No. of Days after the Date of MasterCard Alerts Publication |
|---|---|---|---|
| 1 | 5,000,001 | Unlimited | 60 |
| 2 | 1,000,001 | 5,000,000 | 45 |
| 3 | 10,000[6] | 1,000,000 | 30 |

See the following examples of how the at-risk lengths defined in the table above will be applied in an ADC event.

**Example 1: ADC Event with a Known At-risk Time Frame**

| | |
|---|---|
| At-risk Time Frame—Start Date | 02/01/09 |
| At-risk Time Frame—Known End Date | 03/31/09 |
| MasterCard Alerts Publication Date | 03/01/09 |
| Number of Accounts in the MasterCard Alerts | 500,000 |
| At-risk Length | 30 Calendar Days from the date of the alert |

**Example 2: ADC Event with an Unknown At-risk Time Frame**

| | |
|---|---|
| At-risk Time Frame—Start Date | 03/01/08 |
| At-risk Time Frame—Calculated End Date | 03/31/09 |
| MasterCard Alerts Publication Date | 03/01/09 |
| Number of Accounts in the MasterCard Alerts | 500,000 |
| At-risk Length | 30 Calendar Days from the date of the alert |

- Incremental Counterfeit Fraud Calculation

6. MasterCard reserves the right to invoke FR for cases that are less than 10,000 accounts.

©2009–2011 MasterCard. Proprietary. All rights reserved.

MasterCard will determine the incremental fraud amount by calculating the amount of fraud for a specific ADC event by parent ICA and then reducing the total case-specific counterfeit fraud amount by the average counterfeit fraud experienced by the issuing parent ICA before the at-risk time frame for the ADC event.

- Duplicate Accounts
  The incremental fraud amount is reduced to exclude counterfeit fraud losses on unique accounts that were published in previous MasterCard Alerts within the prior six months.

- Soft Reissue & Chargeback Deduction
  MasterCard considers a soft reissue as a re-issued payment card with the same account number but with a new expiration date and CVC 2 code. The FR program uses a three percent factor for soft reissue. The three percent of the incremental fraud amount is added back into the FR total.

  The chargeback deduction represents the issuers' ability to charge back transactions. A 13 percent deduction will be applied to the incremental fraud amount.

## 6.4.2 ADC Fraud Recovery—Administrative Fee

MasterCard will retain a five percent administrative fee to cover costs associated with managing the FR program.

The updated pricing amounts associated with the FR administration fee are shown in the following table.

**Table 6.3 FR Administrative Fee**

| Pricing | Country | Billing Event |
|---|---|---|
| 5% | U.S. | 2SC1215 |
| 5% | Brazil | 2SC1215 |

The fee will be taken from the final fraud recovery amount and will be identified on the issuer's billing statement under one of the following billing event IDs.

## 6.4.3 ADC Fraud Recovery—BIN Reports

MasterCard offers an optional report that details ADC FR reimbursement amounts at the Parent, Child, and BIN level. The FR BIN Level Report is available at no cost.

To obtain a copy of this report, the issuer must send an e-mail message to account_data_compromise@mastercard.com with the following information:

- Parent ICA number
- MasterCard Alerts Case Number
- Issuer's Contact Name and Phone Number

©2009–2011 MasterCard. Proprietary. All rights reserved.

- Indication of whether this is a one-time request or whether this report should be provided every time FR is invoked for an ADC case

The BIN Level reports will provide FR totals by parent ICA, child ICA, and BIN. Consequently, the issuer (parent ICA) will have a detailed report showing the number and type of accounts reimbursed. The report will provide information similar to the following table.

**Table 6.4 Fraud Recovery**

| Parent ICA | Child ICA | BIN | Total Fraud Recovery Amount USD |
|---|---|---|---|
| NNNN | | | |
| | | NNNNNN | 10.00 |
| | | NNNNNN | 13.00 |
| | | **Subtotal** | 23.00 |
| | NNNN | NNNN | |
| | | NNNNNN | 10.00 |
| | | NNNNNN | 13.00 |
| | | **Subtotal** | 23.00 |
| | NNNN | | |
| | | | 10.00 |
| | | | 13.00 |
| | | **Subtotal** | 23.00 |
| | | **Grand Total** | **69.00** |

## 6.4.4 ADC Fraud Recovery—Reimbursement Notification

Once the final ADC operational reimbursement is calculated on a specific ADC event, MasterCard will notify the responsible acquirers by letter of their financial responsibility. MasterCard will debit the acquirer's MCBS account for the amount calculated.

MasterCard will notify each issuer by e-mail to the parent ICA Security Contact (as defined in the MIM) of the total fraud recovery amount it will receive for a specific ADC event and the date that the fraud recovery amount will be credited to the issuer's MCBS account. See the "Acquirer Responsibility Pre-estimate Letter" sample in Appendix E, Acquirer Responsibility Pre-estimate Letter.

©2009–2011 MasterCard. Proprietary. All rights reserved.

## 6.4.5 ADC Fraud Recovery—Acquirer Responsibility Cap

Section 10.2.4.3 of the MasterCard *Security Rules and Procedures* manual states that MasterCard "may limit compensation" regarding an ADC event. MasterCard will evaluate the following factors to determine whether a responsibility cap is to be invoked for an ADC event:

- Compromised entity PCI Level
- Annual MasterCard sales volume
- Items noted in section 10.2.4.2 of the *Security Rules and Procedures* manual

MasterCard will exercise discretion to determine whether to limit acquirer financial responsibility if an ADC event is determined to have resulted from a system weakness at or associated with a PCI Level 3 or 4 merchant.

At the time MasterCard determines compensation for an ADC event will be limited, MasterCard will work closely with the responsible member and publish a GSA notifying the affected issuers.

The cap is applied to the total FR responsibility and is not applied to any other fees associated with an ADC event.

If MasterCard determines a limit for acquirer financial responsibility, the cap is five percent.

**Merchant Cap Example**

| MasterCard Merchant Annual Sales | 5% of merchant's MasterCard sales | Revised Total FR Responsibility with Cap Applied |
|---|---|---|

The revised acquirer responsibility total is spread to all issuers according to the percentage of their compromised accounts in the ADC event. For example, an ADC event has three issuers, and their portion of the compromised accounts breaks down as follows.

| | |
|---|---|
| Initial Acquirer responsibility (FR) | USD 39,000 |
| MasterCard Merchant Sales | USD 50,000 |
| PCI Cap 5 percent | USD 2,500 |

©2009–2011 MasterCard. Proprietary. All rights reserved.

The revised acquirer responsibility total is spread proportionally to all issuers according to the percentage of their originally calculated reimbursement. The following tables demonstrate how the cap is applied to issuers' pay out.

| | Initial Issuer Pay Out | Issuer Pay Out with Cap Applied |
|---|---|---|
| Issuer 1 – 90% | USD 35,100 | USD 2,250 |
| Issuer 2 – 5% | USD 1,950 | USD 125 |
| Issuer 3 – 5% | USD 1,950 | USD 125 |
| Total | USD 39,100 | USD 2,500 |

©2009–2011 MasterCard. Proprietary. All rights reserved.

# Chapter 7 Financial Settlement

*This chapter describes financial settlement of losses encountered as a result of an ADC event, including operational reimbursement, fraud recovery, and ADC event case management.*


7.1 Overview ..... 7-1

7.2 Operational Reimbursement Notification ..... 7-1

7.3 Operational Reimbursement—Responsible Member Responsibility ..... 7-1

7.4 Operational Reimbursement Billing Event Codes ..... 7-1

7.5 Fraud Recovery—Reimbursement Notification ..... 7-2

7.6 Fraud Recovery—Responsible Member Responsibility ..... 7-2

7.7 Fraud Recovery Billing Events ..... 7-2

7.8 Event Case Management ..... 7-3


©2009–2011 MasterCard. Proprietary. All rights reserved.

# 7.1 Overview

# 7.2 Operational Reimbursement Notification

MasterCard will credit the issuer's MCBS account with the total ADC operational reimbursement payout for each parent ICA number.

If an issuer wants to see a breakdown of the fraud recovery calculated at the bank identification number (BIN) level, MasterCard will provide a report at the BIN level upon request and debit the issuer's MCBS account for a fee associated with providing this service. For more information, refer to section 6.3.3 ADC Operational Reimbursement—BIN Reports

# 7.3 Operational Reimbursement—Responsible Member Responsibility

MasterCard will notify the member deemed responsible for the operational costs that issuers incurred as a result of an ADC event when the operational reimbursement calculations are finalized. A notice will be sent to the acquirer deemed responsible for the ADC event.

# 7.4 Operational Reimbursement Billing Event Codes

Upon completion of the OR process, MasterCard will debit the responsible member, using MCBS; subsequently, MasterCard also will credit issuers through MCBS. The debits and credits will appear on the weekly MCBS billing statement. Detailed below are the billing event codes associated with operational reimbursement debits and credits.

| Billing Event | MCBS Statement Description |
|---|---|
| 2PN-CRD2325 | ADC—Credit for Operational Reimbursement |
| 2SC1327 | ADC—Debit for Operational Reimbursement |

©2009–2011 MasterCard. Proprietary. All rights reserved.

# 7.5 Fraud Recovery—Reimbursement Notification

MasterCard will credit the issuer's MCBS account with the total ADC fraud recovery payout for each parent ICA number.

If an issuer wants to see a breakdown of the fraud recovery calculated at the bank identification number (BIN) level, MasterCard will provide a report at the BIN level upon request and debit the issuer's MCBS account for a fee associated with providing this service. For more information, refer to section 6.4.3 ADC Fraud Recovery—BIN Reports.

# 7.6 Fraud Recovery—Responsible Member Responsibility

MasterCard will notify the responsible acquirers of their responsibility as a result of an ADC event when the fraud recovery calculations are finalized. A letter will be sent to the acquirer responsible for the ADC event.

Section 10.2.2 of the *Security Rules and Procedures* manual defines the rules governing the responsibility associated with an ADC event.

# 7.7 Fraud Recovery Billing Events

Upon completion of the FR process MasterCard will debit the responsible member using MCBS; subsequently, MasterCard also will credit issuers through MCBS. The debits and credits appear on the weekly MCBS billing statement. Following are the detailed billing event codes associated with fraud recovery debits and credits.

The following table shows ADC FR codes that appear on the MCBS statement.

| Country/Region | MCBS Billing Event ID | Description |
|---|---|---|
| U.S. | 2SC1214 | US Debit (Acquirer) |
| Brazil | 2SC1214 | Brazil Debit (Acquirer) |
| U.S. | 2SC-CRD1214 | US Credit (Issuer) |
| Brazil | 2SC-CRD1214 | Brazil Credit (Issuer) |

©2009–2011 MasterCard. Proprietary. All rights reserved.

# 7.8 Event Case Management

The *Security Rules and Procedures* section 10.2.4.6 addresses investigative costs associated with an ADC event.

The following table shows the case management fee structure.

**Table 7.1 Case Management Fee Structure**

| Tier | Minimum No. of Accounts | Maximum No. of Accounts | Billing Event Code (USD) | Billing Event Code (EUR) | Billing Event Code (Reals) | Fee (USD) | Fee (EUR) | Fee (Reals) |
|---|---|---|---|---|---|---|---|---|
| | *Acquirer Investigation* | *Acquirer Investigation* | 2SC1208 | 2KS1208 | 2SC1208 | 500 | 500 | 1,300 |
| 6 | 0 | 9,999 | 2SC1213 | 2KS1213 | 2SC1213 | 2,500 | 2,500 | 6,500 |
| 5 | 10,000 | 99,999 | 2SC1212 | 2KS1212 | 2SC1212 | 7,500 | 7,500 | 19,500 |
| 4 | 100,000 | 999,999 | 2SC1211 | 2KS1211 | 2SC1211 | 40,000 | 40,000 | 105,000 |
| 3 | 1,000,000 | 4,999,999 | 2SC1210 | 2KS1210 | 2SC1210 | 100,000 | 100,000 | 265,000 |
| 2 | 5,000,000 | 14,999,999 | 2SC1209 | 2KS1209 | 2SC1209 | 150,000 | 150,000 | 400,000 |
| 1 | 15,000,000 | >15,000,001 | 2SC1216 | 2KS1216 | 2SC1216 | 250,000 | 250,000 | 650,000 |

©2009–2011 MasterCard. Proprietary. All rights reserved.

# Appendix A Required ADC File Format

*This appendix provides the defined file format and layout for submitting account data to MasterCard for all methods of file submission.*

Required ADC File Format.....A-1

©2009–2011 MasterCard. Proprietary. All rights reserved.

# Required ADC File Format

Following is the defined file format and layout for submitting account data to MasterCard for all methods of file submission. The only required field in the file format is the account number; all other fields are optional. MasterCard requests all the data in the format defined below, for fraud analysis, but will accept the account number only, if additional data is not available.

**NOTE**

**MasterCard requests that the members submit all files as a Microsoft Excel® (*.xls) or text (*.txt) file.**

| Field | Position | Length | Description |
|---|---|---|---|
| Primary Account Number (PAN) | 1–19 | 19 | **Required**, numeric; left-justified; trailing spaces |
| Expiration Date | 20–23 | 4 | **Optional**, YYMM |
| Transaction Amount | 24–35 | 12 | **Optional**, Numeric; right-justified; leading zeros; in currency of transaction |
| Transaction Date | 36–43 | 8 | **Optional**, YYMMDD—Date the transaction occurred |
| MCC | 44–47 | 4 | **Optional**, Must be a valid MCC as defined in the MasterCard *Quick Reference Booklet* [1] |
| POS Entry Mode | 48–49 | 2 | **Optional**, Numeric codes indicating the entry mode of the PAN into the interchange system. Refer to the *Customer Interface Specification* [1] manual for values. |
| Issuer Customer Number (member ID/ICA number) | 50–56 | 7 | **Optional**, Numeric; right-justified; leading zeros |
| Acquirer Customer Number (member ID/ICA number) | 57–63 | 7 | **Optional**, Numeric; right-justified; leading zeros. |
| Merchant ID | 64–78 | 15 | **Optional**, Alphanumeric; left-justified; add trailing spaces. Unique merchant identifier |

1. The manual is available in the Member Publications product on MasterCard OnLine.

©2009–2011 MasterCard. Proprietary. All rights reserved.

| Field | Position | Length | Description |
|---|---|---|---|
| Merchant Name | 79–100 | 22 | **Optional**, Alphanumeric; left-justified; add trailing spaces. Name of the card acceptor ("Doing Business As" name). |
| Merchant City | 101–113 | 13 | **Optional** Alphanumeric; left-justified |
| Merchant State/Province | 114–116 | 3 | **Optional**, Left-justified; trailing spaces |
| Merchant Country | 117–119 | 3 | **Optional**, Must be a valid three-character, alphabetic country code as defined in the *Quick Reference Booklet* [1] |
| Terminal ID | 120–127 | 8 | **Optional**, Unique code identifying a terminal at the card acceptor location (merchant); must be unique within the terminal-owning organization |

©2009–2011 MasterCard. Proprietary. All rights reserved.

# Appendix B Forensic Investigators Approved by MasterCard

*This appendix provides a link to the PCI Security Standards Web site, which identifies PCI-approved PFIs.*

Forensic Investigators Approved by MasterCard.....B-1

©2009–2011 MasterCard. Proprietary. All rights reserved.

# Forensic Investigators Approved by MasterCard

This appendix provides the following link to the PCI Security Standards Web site, which identifies PCI-approved PCI Forensic Investigator (PFIs).

https://www.pcisecuritystandards.org/approved_companies_providers/pfi_companies.php

©2009–2011 MasterCard. Proprietary. All rights reserved.

# Appendix C ADC Event Status Report

*This appendix provides a sample report for the weekly ADC event reporting. These forms can be copied or printed.*

ADC Event Status Report ..... C-1

ADC Investigation Weekly Status Report ..... C-1

©2009–2011 MasterCard. Proprietary. All rights reserved.

# ADC Event Status Report

This form is a sample report for ADC event weekly reporting. These forms can be copied or printed when providing a report to the MasterCard fraud investigator.

This form may change from time to time. The most current version of the form should always be used and is available in this user guide, which will remain available through the MasterCard OnLine® Member Publications Web site.

# ADC Investigation Weekly Status Report

**Date:** _____

**Case Number:** _____

| | |
|---|---|
| **Acquirer Contact Information** | |
| Contact Name | |
| Contact Phone Number | |
| **Alternate Acquirer Contact** | |
| Contact Name | |
| Contact Phone Number | |
| **Compromised Entity Information** | |
| Merchant (or Agent) Name | |
| Location | |
| QIRA Engagement Date | |
| QIRA Onsite Date | |
| Preliminary Report Estimated Date | |
| Final Report Estimated Date | |
| **New Investigation Findings** | |
| For Example<br>MasterCard account count to-date—Track Data, PAN only (or Status of Scans for MasterCard account data, e.g., 50% complete, etc.) | |
| **Other Updates/Comments** | |

©2009–2011 MasterCard. Proprietary. All rights reserved.

Please forward the secured completed status report by e-mail to account_data_compromise@mastercard.com, to the attention of the investigator managing the case.

©2009–2011 MasterCard. Proprietary. All rights reserved.

# Appendix D Incident Report

*This appendix provides a template which is suggested for use when initiating an ADC event to the MasterCard Alerts as noted in Chapter 2.*

Incident Report ..... D-1

©2009–2011 MasterCard. Proprietary. All rights reserved.

# Incident Report

This template is suggested for use when initiating an ADC event to the MasterCard Alerts as noted in Section 2.

| | |
|---|---|
| **Overview** | |
| Date of Report: | |
| Contact Name: | |
| Contact Phone: | |
| Principal Member ID/ICA number: | |
| Provide a description of the incident | |
| **Entity Descriptions** | |
| Name (*If a merchant, provide complete address*): | |
| Address: | |
| City: | |
| State/Province: | |
| Postal Code | |
| Country: | |
| If a merchant, are there additional merchant locations? If so, please provide a list of merchant locations. | |
| Current acquirer name: | |
| Principal Member ID/ICA number: | |
| If a merchant, date merchant initially processed with current acquirer. | |
| Last processing date (if applicable) | |
| Entity PCI Level (For example, Level 1-4): | |
| Number annual incoming transactions: | |
| Is the entity PCI-Compliant? (If so, please provide PCI compliance documentation): | |
| **Potential Compromise Description** | |
| What card data was compromised? | |
| What data elements are at risk? (For example, Name, Address, Account Number, Full Track, Expiration Date, CVC 2, PIN) | |

©2009–2011 MasterCard. Proprietary. All rights reserved.

| Network and Payment Application Description | |
|---|---|
| Does the entity have connectivity to the Internet? | |
| If so, please indicate the type of connection (For example, cable modem, DSL) | |
| Does the entity have wireless/remote access connectivity? | |
| If so, please list the names of people who have access: | |
| List the names of compromised point-of-sale (POS) systems: | |
| What software and version was the entity running at the time of the event? | |
| Was the entity storing track 1 or track 2 data? | |
| Was the entity storing CVC 2 data? | |
| **Answer the following questions only if an e-commerce merchant** | |
| If a merchant, indicate the entity's Web hosting company. | |
| If a merchant, indicate the server type of the entity's e-commerce Web site. | Shared or Dedicated |
| Does the Web hosting company have access to payment card data? | |
| If a merchant, provide the name of the shopping cart application being used. | |
| If a merchant, provide the name of the entity's payment processor or gateway provider. | |
| Select the appropriate storage of the card payment data: | Server<br>Database<br>Payment Gateway<br>Other: |
| **Other Information** | |
| Was the law enforcement notified? | |
| If so, provide the name of the department and agency. | |
| What steps have been taken to remediate the risk/vulnerabilities? | |

©2009–2011 MasterCard. Proprietary. All rights reserved.

Please attach a diagram of your processing flow and include any additional necessary information concerning the investigation, the remediation, or your systems.

The *Account Data Compromise (ADC) Reporting Form* may be accessed through this link.

©2009–2011 MasterCard. Proprietary. All rights reserved.

# Appendix E Acquirer Responsibility Pre-estimate Letter

*This appendix provides the template to use for writing an acquirer responsibility pre-assessment letter*

Acquirer Responsibility Pre-estimate Letter..... E-1

©2009–2011 MasterCard. Proprietary. All rights reserved.

# Acquirer Responsibility Pre-estimate Letter

Senior Business Leader
Fraud Investigations

**MasterCard Worldwide**
Payment System Integrity
2200 MasterCard Blvd
O'Fallon, MO 63368, USA

Internet Home Page: http://www.mastercard.com

[Date]

*Via e-mail: [Acquirer E-mail Address]*

[Acquirer Security Contact Name]
[Acquirer Security Contact Title]
[Acquirer Name]
[Acquirer Address Line 1]
[Acquirer Address Line 2]
[City, State/Province, Zip code, Country]

**POTENTIAL ACCOUNT DATA COMPROMISE EVENT RESPONSIBILITY**
**MC ALERTS CASE # MCANNNN-YY**

Dear [Acquirer Security Contact Name]:

The purpose of this letter is to provide [acquirer name] with a preliminary financial estimate regarding the above-referenced potential Account Data Compromise (ADC) event currently being investigated by MasterCard Fraud Investigations. As the acquirer of record, the potential financial responsibility may be your responsibility as defined in section 10.2.4 of the MasterCard *Security Rules and Procedures* manual. Actual responsibility will be determined after all relevant information about the potential Account Data Compromise event has been examined. The current estimated operational reimbursement and fraud recovery calculated to date for this event is detailed in the table below:

| | **Estimated Responsibility** |
|---|---|
| Operational Reimbursement | USD |
| Fraud Recovery | USD |
| **Total** | USD |

MasterCard has issued this notification in an effort to provide [acquirer name] with timely information.

©2009–2011 MasterCard. Proprietary. All rights reserved.

Please note that this letter sets forth an estimate only and the estimate is only with regard to a potential operational cost reimbursement and potential fraud recovery. This letter does not address any other potential fees, assessments or the like that may relate to or arise in connection with the above referenced potential ADC event.

MasterCard values its relationship with [acquirer_name]. MasterCard is committed to enforcing data security standards for the protection of cardholder information throughout the transaction life cycle. We trust (Acquirer name) supports our initiatives to ensure that all participants, including merchants, vendors, and processors, effectively safeguard and secure payment account data.

Sincerely,

Senior Business Leader

Cc: Acquirer Primary Contact
MasterCard Customer Security and Risk Services Representative
MasterCard Acquirer Account Representative

©2009–2011 MasterCard. Proprietary. All rights reserved.

# Appendix F MasterCard Resources

*This appendix provides information and data requirements the ADC program needs for the accurate submission and maintenance of member, merchant, DSE, or TPP data for aspects of the ADC process.*


MasterCard Information Manual ..... F-1

Quarterly Member Reporting ..... F-1

MasterCard Registration Program (MRP) ..... F-1

System to Avoid Fraud Effectively (SAFE) ..... F-1

MasterCard OnLine ..... F-2

MasterCard Alerts ..... F-2

MasterCard Magnetic Stripe ADC At-risk Accounts Alerts Service ..... F-2


©2009–2011 MasterCard. Proprietary. All rights reserved.

# MasterCard Information Manual

The *MasterCard Information Manual* (MIM) contains member contact information.

The operational reimbursement and fraud recovery applications use the *MasterCard Information Manual* through MasterCard OnLine® to obtain the contact information that is used to communicate with affected issuers and acquirers when communicating details pertaining to an ADC event or potential ADC event. Members must perform a periodic review and update of the Primary Contact and Security Contact name, address, e-mail address, and phone number.

For questions concerning the access and update of ICA number profile in the *MasterCard Information Manual*, please contact the Customer Operations Services team, Technical Account Manager, or Regional Security Representative.

# Quarterly Member Reporting

QMR stands for Quarterly MasterCard Reporting. MasterCard, Cirrus, or Maestro principal customers are required to report performance data to MasterCard on a quarterly basis. Reporting is done through on-line forms that can be found in the MasterCard OnLine® portal, QMR Direct.

The Operational Reimbursement program uses data each issuer provides through the Quarterly Member Report (QMR) to determine the issuing volume for each ICA. The issuer volume is used to associate the issuer with a specific card reimbursement cost when accounts are compromised.

# MasterCard Registration Program (MRP)

The MRP is a mandatory program that requires members to register entities that provide program services to the member and certain types of merchants. Refer to Chapter 9 of the MasterCard *Security Rules and Procedures* manual for more information regarding the MRP.

# System to Avoid Fraud Effectively (SAFE)

SAFE is a database that maintains a repository of fraudulent transactions with fraud types submitted by issuers. MasterCard requires issuers to report to SAFE, at the member ID level, all MasterCard transactions that the issuer considers to be fraudulent, even if the corresponding accounts are not closed or not statused as fraud.

©2009–2011 MasterCard. Proprietary. All rights reserved.

# MasterCard OnLine

MasterCard OnLine is the MasterCard information portal (communication delivery platform) for delivering business tools and secure communications capabilities to members worldwide. Core services and various PC-based tools are available on MasterCard OnLine.

Members must register for access to MasterCard OnLine to use the MasterCard Alerts application. MasterCard OnLine registration is free by navigating the Internet browser to www.mastercardonline.com and selecting the **Enroll Now** link to begin the registration process.

# MasterCard Alerts

MasterCard Alerts is the program that MasterCard uses to notify issuers when MasterCard receives notification that an issuer's accounts are compromised or potentially compromised. MasterCard Alerts contains a narrative of the compromise event and provides each issuer with a list of its cardholder accounts compromised or potentially compromised. The MasterCard Fraud Investigations team uses MasterCard Alerts to store related security bulletins and security contact information, and to track issuer-reported potential ADCs.

For questions regarding MasterCard Alerts, please contact the Customer Operations Services team or your Regional Customer Security and Risk Services representative.

# MasterCard Magnetic Stripe ADC At-risk Accounts Alerts Service

The MasterCard Track Data ADC At-Risk Accounts Alerts™ service seeks to provide issuers with the earliest possible notice of account numbers that MasterCard analysis indicates have a higher risk of fraudulent transactions. Issuers using this service benefit by receiving potentially compromised account numbers as soon as a potential ADC is identified by MasterCard. Issuers can protect their cardholders and themselves against fraud losses rather than waiting weeks or months before confirming that skimming or other improper activity has occurred.

MasterCard algorithms identify merchant locations transacting a disproportionate number of accounts subsequently used in counterfeit card transactions as well as SAFE-reported counterfeit fraud transactions. MasterCard initiates acquirer investigations of the more compelling merchant locations found using these algorithms.

The MasterCard Track Data ADC At-risk Accounts Alerts service is offered on a subscription basis. At this time there is no fee for this service. To enroll in this service, the member should send its contact information and ICA(s) to mastercard_alerts_administrator@mastercard.com

©2009–2011 MasterCard. Proprietary. All rights reserved.

# Appendix G MasterCard Alerts and ADC Reporting Form Field Definitions

*This appendix provides a list of fields on Section A, Page 1 of the ADC Form and their descriptions.*

Section A, Page 1—Field Descriptions ..... G-1

Section A, Page 2—Field Descriptions ..... G-2

©2009–2011 MasterCard. Proprietary. All rights reserved.

# Section A, Page 1—Field Descriptions

The following is a list of fields on Section A, Page 1, and their descriptions.

| Member Information | |
|---|---|
| **Field Title** | **Field Description** |
| MasterCard Alerts User Name | MasterCard Alerts automatically populates this field with the name of the user logged in to the application. |
| MasterCard Alerts User ID | MasterCard Alerts automatically populates this field with the user ID of the user logged in to the application. |
| E-mail Address | MasterCard Alerts automatically populates this field with the e-mail address of the user as it appears in his or her MasterCard OnLine® profile. |
| All required fields are denoted with an asterisk within Section A. | |
| *ICA number | If your MasterCard Alerts profile contains only one ICA, that ICA will be shown. Otherwise, click on the selection button ▼ , and then select the ICA you want to use for this report or type in the ICA. |
| Member name/ Processor name | Enter the reporting entity name, such as acquirer or processor name. |
| Contributor Phone | Enter contact phone number including country code (if non–U.S.-based), area code, and number. |
| **Potential ADC Event Details** | |
| ADC Event/ Merchant exact name | Enter the merchant's name as it appears in the clearing record, including the location number of address, if listed. |
| ADC Event/ Merchant ID | Enter Merchant ID as it appears in the clearing record, if known. If reporting a compromise of an ATM, inclusion of its terminal number is required. |
| ADC Event/ Merchant Street Address | Enter street address, if known. If reporting a compromise of an ATM, inclusion of its street address/location is required. |
| City | City where the merchant or ADC event is located. Enter the complete city name. |
| State | State or province where the merchant or ADC event is located |
| Country | Country where the merchant or ADC event is located as it appears in the clearing record |

**NOTE**

**ADC events are location-specific. If a multi-location merchant chain or franchise is reported, a specific location must be given in the ADC Event/Merchant Street Address field.**

©2009–2011 MasterCard. Proprietary. All rights reserved.

# Section A, Page 2—Field Descriptions

The following is a list of fields on Section A, Page 2, and their descriptions.

| | |
|---|---|
| Acquirer ICA number | Enter merchant's acquirer ICA number as it appears in the clearing record. If you are self-reporting, this ICA must be the same as the initiator's ICA number above. |
| **Period of Possible Compromise** | |
| *From | Enter the first date of possible compromise. |
| *To | Enter the last date of possible compromise. |
| *Total number of accounts affected that transacted at this entity/merchant location during the at-risk period: | Enter the number of potentially compromised accounts |
| Total fraud loss (USD) to-date for affected accounts. | If available, enter the amount of fraud losses in USD resulting from this potential compromise. These fraud losses should already have been reported to SAFE. |
| Type of fraud transactions | If available, enter the type of fraud transactions (such as counterfeit or card not present) that were submitted to SAFE for this case. |
| **Provide your suspected type of compromise:** | |
| Skimming | |
| Merchant Breach | |
| ATM Manipulation | |
| Merchant Burglary | |
| Law Enforcement Recovery | |
| Other | |
| **If you are reporting an ADC event and the compromised accounts are available, attach them below. For potential track data (skimming) ADC event at a merchant location, attach genuine MasterCard transactions occurring at the merchant preceding any subsequent counterfeit transactions at other locations. Please note that a minimum of 10 separate MasterCard accounts are required before an investigation can begin.** | |
| Transaction information is provided in attached document. | Selecting this option indicates that the account numbers will be attached to this form in a separate document. |

©2009–2011 MasterCard. Proprietary. All rights reserved.

| | |
|---|---|
| Compromised account numbers or transaction information is attached.<br>Upload File(s) | If available, use this option to upload a file in the required format (Appendix A) by clicking the **Upload File(s)** button and following the directions. Multiple files may be attached if required. If you are an issuer reporting a potential ADC event, genuine transaction data of the accounts later counterfeited must be entered. |

Answer these questions for potential card skimming ADC events only.

**NOTE**

**To qualify as a skimming event, all the genuine transactions identified above must have occurred within 90 calendar days of one another. In addition, the earliest genuine transaction date must have occurred no earlier than 180 calendar days before the entry date of the ADC Reporting Form.**

| | |
|---|---|
| *Have you authorized that the cardholder had physical possession of the cards at the time of the counterfeit transaction? | Yes/No<br>The default value is no. |
| *Have the fraud transactions been reported to SAFE? | Yes/No<br>The default value is no. |
| *Type of fraud transactions | Enter the type of fraud transactions that were submitted to SAFE for this case (such as counterfeit or lost/stolen). |
| Contributor Comments | Enter any additional information not covered elsewhere; contributors of confirmed or potential ADC events can use this box in lieu of an attachment such as an Incident Report (Appendix D). If more than one acquirer may be responsible for a confirmed or potential ADC event, enter that information here. |
| Attachments: | Attach the ADC Investigation Weekly Status Report or the Incident Report form, forensic report, or any other documentation that would help the investigator better understand the event. |

**One of following three options can be chosen when you have finished Section A.**

©2009–2011 MasterCard. Proprietary. All rights reserved.

| | |
|---|---|
| Cancel | Erases all information and attachments from the system with no record of the tracking number. The status is "Cancelled." |
| Save as Draft | Saves the entered information and attachments but does not release the report to MasterCard. The status remains "Draft." |
| Submit | Submits the report to MasterCard. The submitter will no longer have access to the report until MasterCard has reviewed the information. The status becomes "New." |

**NOTE**

**If you leave the Section A input page for any reason, click Save as Draft at the top or bottom of the page to ensure that your information is saved.**

©2009–2011 MasterCard. Proprietary. All rights reserved.

# Appendix H MasterCard Alerts ADC Reporting Form Status Codes

*This appendix explains the ADC Reporting Form status codes used in the ADC Summary.*

MasterCard Alerts ADC Reporting Form Status Codes ..... H-1

©2009–2011 MasterCard. Proprietary. All rights reserved.

# MasterCard Alerts ADC Reporting Form Status Codes

To review the status of any reported ADC event or potential ADC event, the member must navigate to MasterCard Alerts on MasterCard OnLine and select the ADC Summary from the ADC Investigation pod.

The ADC Summary designates one of the following classifications:

- Draft

  Indicates that the data entered in Section A of the ADC Reporting Form was saved but not submitted to MasterCard; often this occurs when required information in the ADC Reporting Form is not present or complete.

- New

  Indicates that the data entered in Section A of the ADC Reporting Form was successfully submitted to MasterCard

- Open

  Indicates that MasterCard has requested that the acquirer or acquirer's agent initiate an investigation of the merchant location

- Investigating

  Indicates the acquirer has completed Section B of the ADC Reporting Form, acknowledging the MasterCard request for an investigation

- Results Submitted

  Indicates the acquirer has completed an investigation and Section C of the ADC Reporting Form has been submitted for MasterCard review

- Pending

  Indicates that the case is in a "pending" status while additional data is prepared. A case may receive a status of "pending" at any time during the investigation process.

- Closed

  Indicates that the issuer's investigation request has been reviewed and that no further investigation will be conducted

If you want to know the status of an investigation request, log onto MasterCard Alerts and access the ADC Summary.

©2009–2011 MasterCard. Proprietary. All rights reserved.

# Appendix I MasterCard Alerts ADC Section C—Investigation Results

*This appendix describes the various fields of MasterCard Alerts Reporting Form Section C.*


Field Definitions ..... I-1
- Merchant Information ..... I-1
- POS Equipment Details ..... I-1
- Investigative Results ..... I-1
- Law Enforcement Contact Information ..... I-1
- Merchant Investigation Results ..... I-2
- Preventive Measures Implemented ..... I-2


©2009–2011 MasterCard. Proprietary. All rights reserved.

# Field Definitions

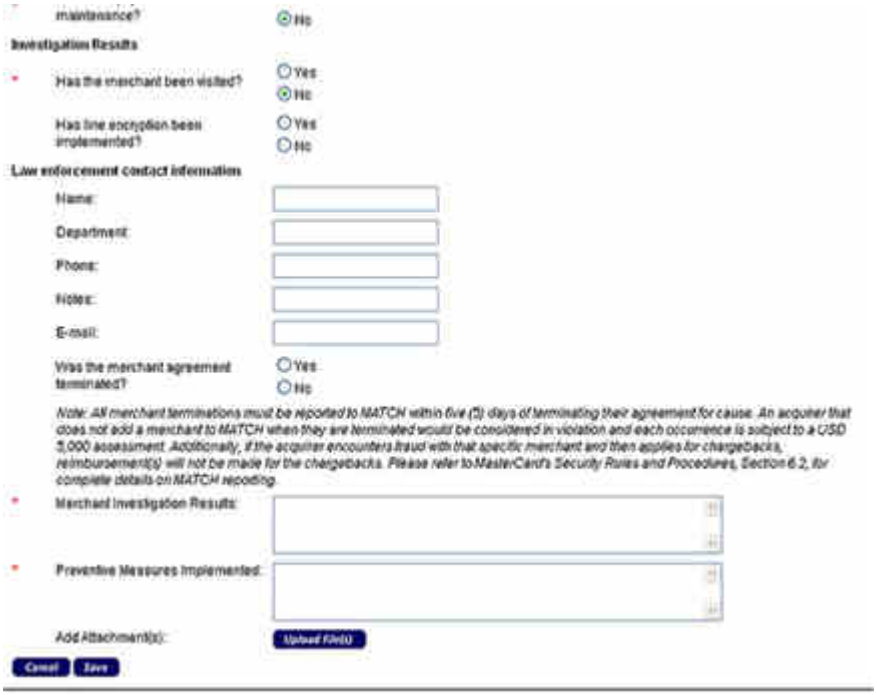
Following are the fields of the MasterCard Alerts Reporting Form C and their definitions.

## Merchant Information

Complete as required.

## POS Equipment Details

Enter information for any POS equipment hardware or software affected by this ADC event. If the information is included in one or more attachments, enter "See attachment" or "No."


maintenance?
No
Investigation Results
Has the merchant been visited?
Yes
No
Has line encryption been implemented?
Yes
No
Law enforcement contact information
Name:
Department:
Phone:
Notes:
E-mail:
Was the merchant agreement terminated?
Yes
No
Note: All merchant terminations must be reported to MATCH within five (5) days of terminating their agreement for cause. An acquirer that does not add a merchant to MATCH when they are terminated would be considered in violation and each occurrence is subject to a USD 5,000 assessment. Additionally, if the acquirer encounters fraud with that specific merchant and then applies for chargebacks, reimbursement(s) will not be made for the chargebacks. Please refer to MasterCard's Security Rules and Procedures, Section 6.2, for complete details on MATCH reporting.
Merchant Investigation Results:
Preventive Measures Implemented:
Add Attachment(s):
Upload File(s)
Cancel
Save

## Investigative Results

Complete as required. MasterCard needs to know whether an on-site visit was made and, if so, who made the visit.

## Law Enforcement Contact Information

Complete as required. MasterCard needs to know whether law enforcement is involved and, if so, how to contact them.

©2009–2011 MasterCard. Proprietary. All rights reserved.

## Merchant Investigation Results

Was the merchant agreement terminated? Indicate whether the merchant agreement or the agency relationship was terminated, for whatever reason. All merchant terminations must be reported to MATCH within five days of terminating the agreement for cause.

Indicate in detail what the investigation findings were. Alternatively, the details can be attached using the **Upload File(s)** button.

## Preventive Measures Implemented

Indicate in detail what preventative measures were implemented to ensure that the ADC activity has ended and how it will be prevented from reoccurring in the future. Alternatively, the details of such measures can be attached by using the **Upload File(s)** button.

MasterCard response requirements are satisfied by clicking the Save button. Clicking the **Cancel** button keeps the results from being saved and requires all the information to be re-entered.

©2009–2011 MasterCard. Proprietary. All rights reserved.